Amendments to the Written Description of the Specification

Applicant presents replacement paragraphs below indicating the changes with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing.

On page 1, after the title insert: --Background Of The Invention--;

On page 1, after "Background of the Invention" but before the first paragraph insert --Field of the Invention--;

On page 1, before the second paragraph beginning on line 10, insert --Discussion of the Related Art--;

Please replace the second paragraph on page 1, lines 7-12 as shown below:

--A common type of ~~attacks of~~ attack against an integrated circuit executing a secured algorithm consists of analyzing the power consumption of the integrated circuit or of the portion thereof executing the algorithm handling secret data. Such power consumption analysis attacks are known as ~~the~~ SPA (single power analysis) or DPA (differential power analysis) and consist of analyzing the power consumption of an integrated circuit according to the data that it processes to discover data meant to be secret.--

On page 2, before line 1, insert --Summary of the Invention--;

Please replace the second and third full paragraphs on page 2, lines 6-10 as shown below:

--The present invention also aims at providing a solution which does not simply translate as ~~in~~ an increase in the possible combinations to be examined by the pirate.

To achieve these and other objects, the present invention provides a method for supplying an asynchronous calculation element of an integrated circuit, ~~consisting of~~ comprising randomly varying the instantaneous supply power of the calculation element.--

Please replace the ninth full paragraph on page 2, lines 24-26 as shown below:

--The foregoing objects, features and advantages of the present invention, will be discussed in detail in the following non-limiting description of specific embodiments in connection with the accompanying drawings~~, in which:~~.--

On page 2, before line 27, insert --Brief Description of the Drawings--;

Please replace the eleventh paragraph, on page 2, lines 27-29 as shown below:

--Fig. 1 ~~very~~ schematically shows in the form of blocks an embodiment of a supply circuit of an asynchronous calculation element according to the present invention; and--

On page 3, before line 1, insert --Detailed Description--;

Please replace the first paragraph on page 3, lines 1-9 as shown below:

--For clarity, only those method steps and circuit elements which are necessary to the understanding of the present invention have been shown in the drawings and will be described hereafter. In particular, the algorithm implemented by the calculation element to be protected has not been ~~detailed and is no object of the present invention,~~ described in detail. ~~the~~ The present invention ~~applying~~ a pplies wh atever the implemented asynchronous process is. Further, the asynchronous calculation element is of course most often associated with other circuit elements with which it is integrated. Reference will only be made hereafter to the asynchronous calculation element and to its power supply, the present invention having no effect upon the rest of the circuit which depends on the application.--

Please replace the three paragraphs beginning on page 3, line 26 through page 4, line11 as shown below:

--Should the application allow for it, especially should it impose no time constraints, then ~~can~~ a random generator be used, which has the advantage of dissociating ~~no~~ not only the supply, but also the duration with respect to the processed data. The processing time is thus made random.

Fig. 1 partially and ~~very~~ schematically shows in the form of blocks an embodiment of a circuit for supplying an element 1 of asynchronous execution of a data processing algorithm (ASYNC-ALGO). Conventionally, the asynchronous calculation element may be schematized as a circuit receiving input data E, providing output data S, and exchanging control signals (CTRL) with the rest of the integrated circuit (for example, with a microprocessor not shown). Among the control signals is especially the signal by which element 1 indicates to the rest of the integrated circuit that output data S are available.

According to the present invention, circuit 1 is supplied by means of a circuit 2 (VAR). Circuit 2 provides a variable power to circuit 1 and is supplied by a voltage Valim, for example, the integrated circuit supply voltage. In the sense of the present invention, the power variation may be performed in voltage or current, while respecting, if need be, the minimum supply

constraints (for example, in voltage level) to avoid loosing the data under processing by asynchronous circuit 1.--

Please amend the third full paragraph on page 4, lines 17-19 as shown below:

--In the case where ~~a~~ the same integrated circuit contains several distinct asynchronous processing circuits, said circuits may be supplied separately from one another or together by means of a same variable generator 2.--

On page 5, line 28, please insert:

--Having thus described at least one illustrative embodiment of the invention, various alterations, modifications, and improvements will readily occur to those skilled in the art. Such alterations, modifications, and improvements are intended to be within and scope of the invention. Accordingly, the foregoing description is by way of example only and is not intended as limiting. The invention is limited only as defined in the following claims and the equivalents thereto.

What is claimed is: --